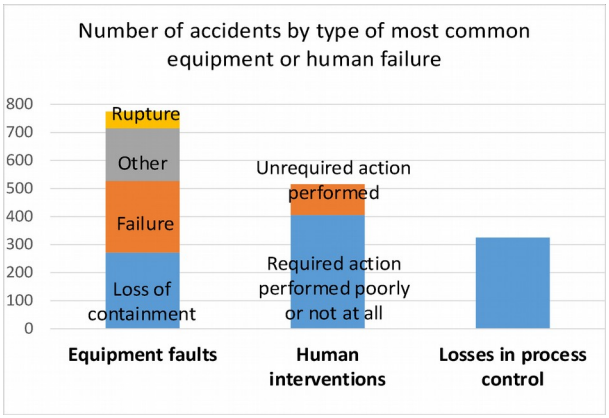
Preventing multiple failures

Since 2016, 25% of accidents in ICPEs (classified facilities for environmental protection requiring authorisation or registration), impacting people and property, have been caused by multiple failures involving equipment faults or human interventions. Most initial post-accident verifications focus on the incriminated system: did it function as intended and were the necessary human actions taken? One failure is already one too many; this is all the more true for multiple failures. It is therefore important to know how to analyse cases of multiple failures accurately and with all the requisite objectivity, as this will guide investigations into the nature of their root causes: were there common modes? were there generic failures? were there failures specific to an isolated system that was insufficiently analysed? were there deeper failures caused by organisational methods? All these clues provide the information needed to help explain the causes of multiple failures and prevent them from recurring.

1. What are the most common multiple failures?

In accidents occurring at ICPEs since 2016, involving multiple failures, the primary cause has been equipment failures (loss of containment, breakdown, rupture). This is followed by human errors and actions that were performed either incorrectly or not at all (misjudgement, misinterpretation, poor decision-making or inappropriate actions) and lastly by losses of process controls (incompatible mixtures, reaction runaway, or parasitic reactions).



Multiple failures can aggravate an initial event, for instance when safeguards designed to limit the severity of a hazard do not work (water curtains that fail to activate, a faulty detector that fails to identify an incident in time...). Some failures in risk control measures may result in major accidents having effects that extend beyond a site's confines: *odours, visual or noise impacts* (*such as a gas alert), and even trigger the implementation of a site's external emergency plan (ARIA 51372 and 52842).*

2. Actions required at various levels to prevent multiple failures

2.1. Is making equipment changes shortly after an accident enough?

Following an event caused by multiple equipment failures, the system containing the defective equipment must be analysed closely. The analysis findings can lead to a number of changes:

- retrofitting of defective equipment, such as changes in valve or detector technology or the fitting of explosive atmospheres certified equipment;
- process control changes, such as ensuring that certain functions are maintained during shutdowns and restarts, and improvements to control mimic panels;
- addition of safety equipment: sensor redundancy, detection/action loops, etc.;
- increased monitoring: CCTV, webcams, more frequent rounds;
- improved system inspection and maintenance, such as changes in the frequencies of inspections, tests, and maintenance plans (*ARIA 47654, 49388, 49575, 50121, 50150).*

To implement these changes, operators must call on skilled people to choose the right equipment and processes. A **study of the ergonomics of a plant's systems** or control rooms can support the choices made *(valve access, availability of information on mimic panels).*
Operators must take a broad view of events, analyse them in depth, and look for potential common failure modes. Because simply retrofitting equipment is not enough, operators must take a hard look at the system that has caused multiple failures as well as any systems that are similar to it or interact with it. It is essential to review their **risk analyses,** identify common causes, and widely implement preventive measures based on these new analyses. The analytical and organisational methods used may also be challenged (*ARIA 50254, 52784, 51220).*

2.2. What resources are necessary to facilitate decision-making?

Despite support from supervisors and maintenance teams, technicians and shift crews sometimes misjudge a situation, or commit errors that lead to unwanted events. When multiple errors occur, organisational factors are always the culprit. Lack of communication may also explain why the right people were not consulted and why inappropriate actions were taken.

ARIA 51220 – 19/09/2017– Aramon (Gard) – France

At 9:20 a.m., a rupture disc of a reactor used to produce an organomagnesium compound burst when the reactor's internal pressure rose too high. The incident was caused by a nonconforming mixture that had formed in the reactor. First, the ambiguous instructions led a technician to add an insufficient amount of initiator. Then, seeing that the reaction had not yet started, a second technician added more reagents.

The process sheet indicated that the reagent could be added after, but only after receiving the supervisor's approval. The operation took place on a Saturday and the chemical engineer belatedly informed the on-duty engineer. This lack of communication between the workers of both shifts and the technicians' lack of experience are what set the stage for the incident. The operator subsequently implemented a number of changes : tracking of technicians who are accredited to carry out synthesis operations has been reinstated ; the process sheet now indicates the amounts of reagent to be added and includes hold points for the start of the reaction ; the reaction may no longer be carried out over the weekend and it must be scheduled at the beginning of a shift so that workers may monitor it from start to finish. In addition, the operator conducted an in-depth review of organomagnesium compound synthesis in order to establish production standards and problem-management guidelines applicable at all its similar production sites.

Cumulated difficulties in making the right decisions when managing incidents can be mitigated by leveraging various organisational strengths:

- **clear procedures and instructions facilitate decision-making:**

The retrofits mentioned earlier often result in updates to the associated procedures and operating instructions:

- improved operating procedures, such as process sheets with hold points for complex operations, quick-response procedures to be used when abnormal situations arise, shutdown/restart procedures, tests, inspections, and maintenance plans;

- improved emergency-response procedures, such as incorporating a new scenario to a site's internal emergency plan, changing the on-duty call procedure, and updating the telephone numbers of external resources.

Analysing events makes it possible to find out what the control-room technicians needed to make the right decisions. Procedures and sheets must be legible, easy to reach and to use by all. To ensure that they are simple to understand, the relevant people and resources must participate in their design. Indeed, some accidents highlight the importance of bringing in various professions and perspectives when drafting these documents. Once written, supervisors and managers at all levels must efficiently work together to ensure that they are systematically implemented (*ARIA 50339, 49109, 52021, 52324, 52384).*

Another aspect that deserves special consideration is control-room ergonomics. The technicians working there should be consulted to find out whether equipment retrofits are appropriate and well designed.

- **put the emphasis back on training and personnel qualification:**

Updating instructions and procedures also requires teaching personnel how to adopt these changes. This entails organising actions such as awareness-raising, training sessions, accreditation (in some cases), knowledge testing, and role-play simulations. It is important to involve contractors in awareness and training courses and, more generally, within a plant's organisation (*ARIA 49970, 50686, 52553).*

Refresher training courses for technicians, especially those regarded as 'experts', should be designed to keep them aware of the reality of the risks of the facilities they operate.

- **efficient workplace organisation, supervision, and communication:**

One way to develop efficient means of communication (*such as safety flashes and safety meetings/confabs*) is to hold a brainstorming session between all the sites in a company or a particular sector of business. The goal is to create and implement long-term communication actions.

All changes must be supported by a solid system for managing modifications and degraded modes. Management as a whole must be the first to adopt the process (*ARIA 51172).*

3. Lasting, in-depth changes

Incidents involving multiple failures remind us that it is important to take an in-depth look at **root causes**, **defence mechanisms** (barrier and risk management measures) and **risk analyses** on the whole. Their lessons make it possible to establish thorough, long-term means of prevention and protection, reduce the recurrence of such incidents, mitigate their consequences, and check the appropriateness of accident scenarios.

Despite this, a decline in vigilance may occur when the number of incidents and accidents drops within a plant. However, improving safety requires constant alertness and attention to **weak signals** or **situations with a high severity potential**. Taken individually, incidents may be of little consequence. But when combined with other circumstances, they can result in extensive damage.

The messages to be delivered must also reach the right people. It is therefore essential to use several methods of communication, such as drawing up success trees (versus causal trees), bringing in a neuroscientist to explain human factors, or investigating **risk perception** at all levels within a plant.